CERTIFIED MAIL™

7005 1820 0007 5636 3739

10/065452

Chung-E Wang
845 West Cove Way
Sacramento, CA 95831

OIPE IAP86
JAN 19 2006
PATENT & TRADEMARK OFFICE

Mr. Ellen C. Tran
Commissioner For Patents
P. O. Box 1450
Technology Center 2134
Alexandria, Virginia 22313-1450
January 12, 2006

RECEIVED
JAN 19 2006
USPTO MAIL CENTER

Jang

10/065452

845 West Cove Way
Sacramento, CA 95831

Mr. Ellen C. Tran
Commissioner For Patents
P. O. Box 1450
Technology Center 2134
Alexandria, Virginia 22313-1450
January 12, 2006

Dear Mr. Tran,

Enclosed is my response to your communication dated October 31, 2005. (Mailing date November 15, 2005). If further information is required, please notify me. Thank you.

Sincerely,

Chung-E Wang

Chung-E Wang
Application No. 10/065,452
Art Unit: 2134

Claim Objections

3. Claims 6 and 7 are objected to because of the following informalities: It appears that claim 6 should have a preamble that it depends from independent claim 5. In addition claim 7, contains two sentences, either another claim should be added or text that relates "a method of introducing randomness into the process or arithmetic coding by changing the order of dividing an interval into smaller interval with an encryption key" to the rest of claim 7 should be added. Appropriate correction is required.

Because of a typo, label [c6] is added automatically by EFS-ABX software. There should be only 6 claims. Correct claims 5 and 6 are as below.

[c5] A method of shuffling the Huffman tree with an encryption key comprised of the following steps:

a) Associate each interior node with a bit of the encryption key.

b) Swap the left child and the right child of an interior node, if the corresponding encryption bit is 1.

[c6] A method of introducing randomness into the process of the arithmetic coding by shuffling the interval table with an encryption key. That is, a method of introducing randomness into the process of the arithmetic coding by changing the order of dividing an interval into smaller intervals with an encryption key.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 1-7 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Each claim teaches solely to the abstract manipulation of data.

The basic idea of my invention is to use well-known, existing compression algorithms to do encryptions. Well-defined steps and instructions for accomplishing simultaneous compression and encryption are given in my specification. They are not just abstract manipulation of data.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-7, are rejected under 35 U.S.C. 102(b) as being anticipated by Barbir U.S. Patent No. 6,122,379 (hereinafter '379).

As my invention, Barbir's idea is to use known, existing compression algorithms to do the encryption. There are two major processes in every compression algorithm, the modeling process and the encoding process. Barbir's idea is to alter the modeling process of the compression algorithm and my idea is to alter the encoding process instead. Altering the modeling process is more time consuming than altering the encoding process. Moreover, altering the modeling process would affect the compression efficacy and altering the encoding process won't.

As to independent claim 1, "A method of introducing randomness into the process of the dictionary encoding of Lampel-Ziv data compression" is taught in '379 col. 7, lines 62-67;

In Claim 1, I introduce the randomness by shuffling the initial values of the dictionary with the encryption key. In '379 col. 7, lines 62-67, Barbir introduces the randomness by updating a modeler's internal state randomly. (So, the probabilities of characters/symbols would be different.)

"by shuffling the initial values of the dictionary with the encryption key" is shown in '379 col. 5, lines 26-33.

In Claim 1, shuffling the initial values of the dictionary with the encryption key doesn't change probabilities of characters/symnols. It only results in a different encoding. In '379 col. 5, lines 26-23, Barbir introduces the randomness by changing the modeler.

As to independent claim 2, "A method for combining a random shuffle with a Lampel-Ziv data compression to achieve a simultaneous data compression and encryption, comprised of the following steps:" is disclosed in '379 col. 7, lines 62-67;

In '379 col. 7, lines 62-67, Barbir claims that his idea of altering the modeling process can be used with different encoding processes. In my Claim 2, I don't change the modeling process of a Lampel-Ziv compression.

"a) use the encryption key to shuffle the initial values of the dictionary randomly" is shown in '379 col. 5, lines 26-33;

In Claim 2, shuffling the initial values of the dictionary with the encryption key doesn't change probabilities of characters/symbols. It only results in a different encoding. In '379 col. 5, lines 26-23, Barbir introduces the randomness by changing the modeler.

"b) compress the input string normally" is taught in '379 col. 11, lines 54-67;

In '379 col. 11 lines 54-67, Barbir claims that his idea can be a building block of a multi-step compression and encryption. My Claim 2 doesn't involve multi-step compression and encryption.

"c) perform the bit-wise XOR operation on the compressed result and the encryption key" is shown in '379 col. 5, lines 26-33 and col. 2, lines 11-23.

As stated in '379 col. 2, lines 11-23, XOR is a well-known operation. My Claim 2 isn't claiming XOR is a new invention. My Claim 2 is claiming that the combination of steps a), b), and c) is a new invention.

As to dependent claim 3, "where step a) is comprised of the following step: a) If the dictionary doesn't have any initial values, initialize the dictionary with a particular set of values and then use the encryption key to shuffle the dictionary" is disclosed in '379 col. 7, lines 22-45.

In '379 col. 7 lines 22-45, Barbir uses a random number generator to determine when to update the modeler's internal state, i.e. probabilities of characters/symbols. In my Claim 3, I use a random number generator to determine the initial values of the dictionary.

As to independent claim 4, "A cryptographic method of concealing information in the process of Huffman coding by altering the Huffman tree with an encryption key" is taught in '379 col. 7, line 62 through col. 8, line 44.

In '379 col 7. line 62 through col. 8 line 44, Barber is claiming that his idea of altering the modeling process can be used with compression algorithms such as LZ compression, RLE, etc. In my claim 4, I change the encoding process (not the modeling process) by altering the Huffman tree with an encryption key.

As to independent claim 5, "A method of shuffling the Huffman tree with an encryption key comprised of the following steps:" " is taught in '379 col. 7, lines 22-67;

In '379 col. 7 lines 22-67, Barbir uses a random number generator to determine when to update the modeler's internal state, i.e. probabilities of characters/symbols. He also claims that his idea can be used with a wide range of compression algorithms such as LZ compression, RLE, etc. In my Claim 5, I use an encryption key to alter the Huffman tree and thus alter the encoding process.

"a) associate each interior node with a bit of the encryption key" is shown in '379 col. 8, lines 36-67.

In '379 col. 8 lines 36-67, Barbir uses an encryption key to determine the initial frequencies (i.e. probabilities) of symbols. In Claim 5, I use an encryption key to alter the Huffman tree. In other words,, Barbir uses an encryption to alter the modeling process and I use an encryption key to alter the encoding process.

As to dependent claim 6, "b) Swap the left child and the right child of an interior node, if the corresponding encryption bit is 1" is disclosed in '379 col. 6, lines 10 through col. 7, line 21.

In '379 col. 6, lines 10 through col. 7 line 21, Barbir describes the general idea of the well-known arithmetic coding and his new modeling method. In this claim, swapping left child with the right child of an interior node doesn't change probabilities of characters/symbols. It only changes the result of the encoding.

As to independent claim 7, "A method of introducing randomness into the process of the arithmetic coding by shuffling the interval table with an encryption key" is taught in '379 col. 6, lines 10 through col. 7, line 21;

In '379 col. 6, lines 10 through col. 7 line 21, Barbir describes the general idea of the well-known arithmetic coding and his new modeling method. In this claim, shuffling the interval table with an encryption key doesn't change probabilities of characters/symbols. It only changes the result of the encoding.

"That is, a method of introducing randomness into the process of the arithmetic coding by changing the order of dividing an interval into smaller intervals with an encryption key" is shown in '379 col. 6, lines 37-55.

In '379 col. 6, lines 37-55, Barbir describes the basic idea of his modeling method. In this claim, changing the order of dividing an interval into smaller intervals with an encryption key doesn't change probabilities of characters/symbols. It only changes the result of the encoding.